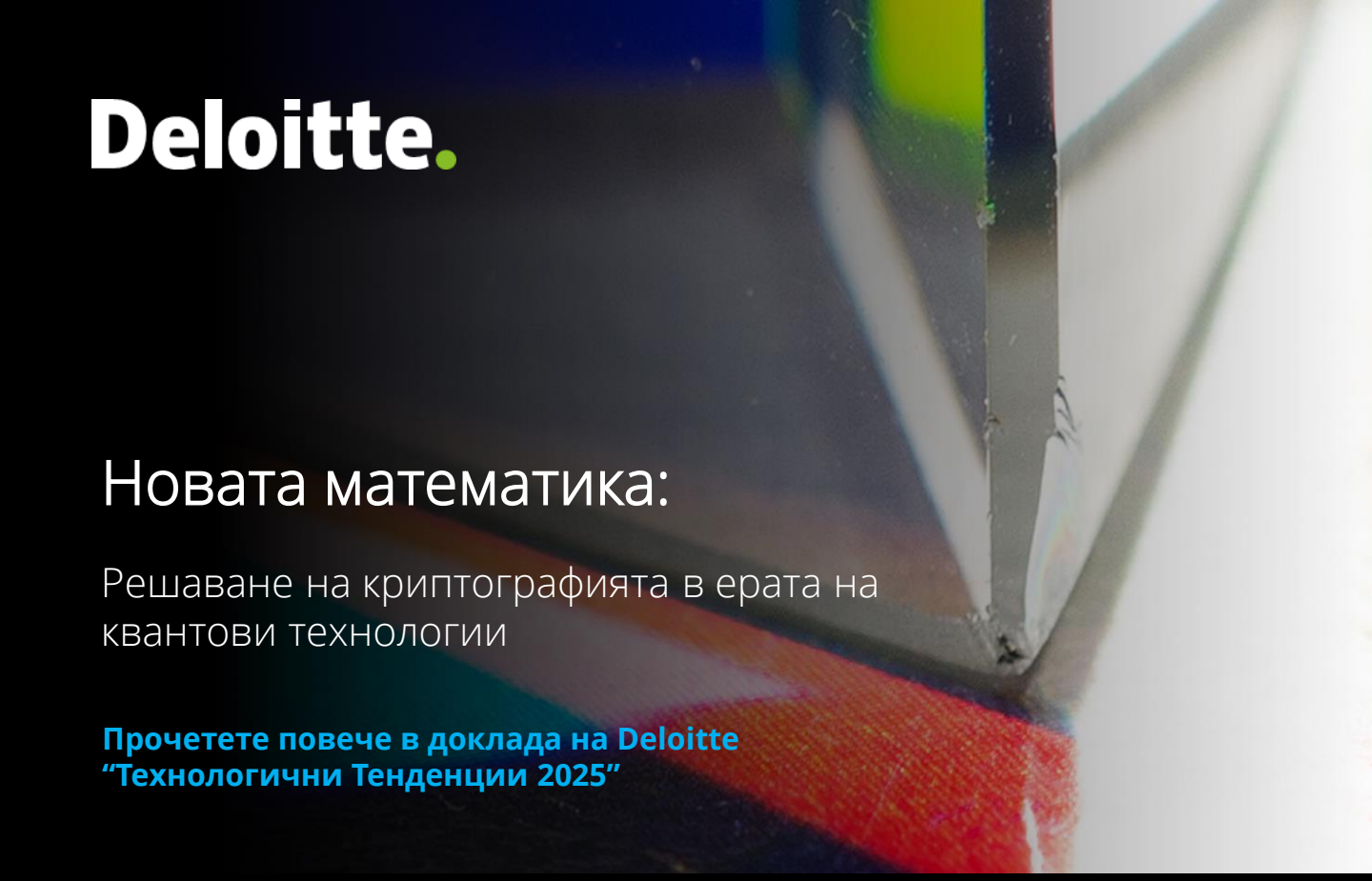

Новата математика:

Решаване на криптографията в ерата на квантови технологии

Прочетете повече в доклада на Deloitte “Технологични Тенденции 2025”

С развитието на основните технологии, благодарение на по-мощния хардуер и иновациите, позволяващи повече изчисления и повишена производителност чрез AI, ИТ организациите трябва да обърнат внимание и на още един критичен фактор, който се задава на хоризонта. Докладите на Deloitte за Технологичните Тенденции в миналото изтъкваха ролята и значението на понятието сигурност като стабилизиращия елемент в технологичния свят.

Опазване на бъдещето в квантовата ера

Днешната зависимост от данните изисква не само изчислителна производителност, но и надеждна защита. Интегритетът на данните е от ключово значение за ефективното управление, като гарант, че AI моделите се обучават върху точна и конкретна информация. Също така конфиденциалността на данните – била тя при преноса им (високоскоростна търговия, диагностично оборудване, IoT полеви данни) или при статичните (резервни копия, финансови модели, транзакционни записи) – е от решаващо значение за стабилността на цифровата ни икономика.

Криптографията – силата зад интегритетът и конфиденциалността, се използва навсякъде. Съвременните широко използвани алгоритми за криптиране се уповават по своята същност на математически задачи (разлагане на големи множители или решаване на дискретни логаритми), които конвенционалните компютри не могат да решат ефективно. Тези традиционни методи за защита на информацията сега биват застрашени от появата на нови технологии като квантовите компютри. Макар и да предлагат безпрецедентни изчислителни способности, те също така и създават значителни рискове за настоящите стандарти за криптиране. Дори браузърите ни използват конкретни стандарти за комуникация, чиято сигурност вече се поставя под въпрос.

Квантовото предизвикателство

Квантовите компютри използват съвсем различна физика – те работят на принципите на квантовата механика, което им позволява да извършват сложни изчисления със скорости, недостижими за класическите компютри. Тази способност обаче заплашва да подкопае сегашните стандарти за криптиране, излагайки на риск поверителни данни. За ръководителите разбирането на последиците от квантовите компютри става от съществена важност, за да защитят организационните си активи и да запазят доверието на заинтересованите страни.

Неотложността на квантово-устойчивата криптография

Квантовите изчисления се развиват с безпрецедентни темпове. Компании като IBM, Fujitsu и Microsoft, а също така и по-малки такива – като Atom, вече изграждат квантови процесори, чиято изчислителна мощ ще засенчи дори най-добрите съвременни задвижвани от графични процесори компютри, които вече работят с над 1000 кюбита на процесор. Нещо повече, нови разкрития на Масачузетският Технологичен Институт (MIT) за свързване на фотони и атоми, ще съкратят времето между изчисленията и отчитането в степен, премахваща едно от ключовите препятствия за растежа на квантовите технологии.

Защо това е важно?

Притеснението е, че днешните стандарти, които са вече с широко приложение, не могат да бъдат променени лесно. Някои организации, поради това, че техният технологичен пакет е бил изграждан през годините, все още предлагат да се използват по-ниски стандарти, които или не изискват голяма изчислителна мощност на крайните устройства, или са несъвместими с техния остаряващ технологичен пакет.

В същото време прогнози сочат, че криптографски-значимите квантови компютри (CRQC) могат да разбият текущите методи за криптиране още през 30-те години на века. Някои доклади дори предполагат, че китайски квантови машини може би вече са компрометирали базови алгоритми, което може да подкопае дори най-силните стандарти за криптиране като AES.

Пътят към решенията

За щастие вече се появяват решения. Разработват се пост-квантови криптографски алгоритми (PQC), препоръчани от NIST, които осигуряват сигурно опаковане на ключове и цифрови подписи, като в момента се разработват и още иновации. Както се посочва в Tech Trends 2025: „Актуализираните стандарти на NIST се отдалечават от днешните математически задачи с голям на брой разлагания на множители и залагат на използването на решетки и хеш-функции – задачи, достатъчно сложни, за да затруднят дори квантовите компютри.“

Все пак, макар че квантовите компютри, способни да разбиват днешното криптиране, могат да се появят до 5-10 години, преходът към квантово-устойчиви системи може да отнеме също толкова дълго, създавайки „рисков прозорец“, особено предвид възможността за нападателите да събират криптирани днес данни, за да ги декриптират по-късно (атаки от типа “harvest now, decrypt later” – англ. „събиране сега, декодиране по-късно“). За разлика от кризата Y2K, при която рискът беше ограничен във времето и от части предсказуем, времевата рамка за CRQC остава несигурна, което кара много организации да не приоритизират подготовката, въпреки потенциално огромното въздействие.

Бизнес-последиците и планът за действие

За да се справят с тази заплаха, организациите трябва проактивно да започнат да преминават към квантово-устойчиви криптографски алгоритми, които могат да издържат на възможностите на квантовите машини. Това включва:

- **Инвентаризация на всички криптографски алгоритми**, които са в употреба.
- **Оценка на предизвикателствата** при внедряване на нови квантово-устойчиви решения.
- **Планиране на ъпгрейди** на хардуер и софтуер за своевременно смекчаване на последиците.
- **Инвестиране в квантово-устойчиви алгоритми** за защита от бъдещи атаки.
- **Сътрудничество с експерти по киберсигурност** за изграждане на надеждни стратегии за сигурност.

Ангажираността на Deloitte към квантовата сигурност

Deloitte предоставя стратегически насоки, подкрепа за внедряване и текущо наблюдение, за да помогне на организациите да се адаптират към квантовите предизвикателства. Като си партнират с експерти, компаниите могат да си осигурят сигурна цифровизирана среда и за напред.

Заключение

Въпреки че квантовите компютри обещават огромни ползи – като например ускоряване откриването на лекарства чрез симулиране на сложни молекули – те също така поставят и безпрецедентни предизвикателства пред сигурността. Като възприемат квантово устойчива криптография, предприятията могат да защитят своите данни и да запазят доверието в дигиталната ера.

Приемете този стратегически подход не само като една техническа необходимост, но и като инвестиция в бъдещия организационен интегритет.

Можете да разгледате 16-тия годишен доклад на Deloitte и да се запознаете с най-новите тенденции тук: Tech Trends 2025 | Deloitte Insights.